#6


Title: ELECTRONIC HIGH-SECURITY SAFE LOCK

Inventor: Ahmed Raslan

## FIELD OF THE INVENTION

This invention relates to electronic controlled locks and specifically to high security multi-user safe door locks.

## BACKGROUND

Banks and certain business establishments have a need for very secure safes. In these circumstances a high security safe may be appropriately accessed by more than one person. Often, repeated access by a number of trusted employees and officers of the institution is required for efficient conduct of the business.

Large high security safe installations are typically set within thick hardened steel vault enclosures that include massive or roller-mounted steel doors. These massive doors often require considerable force to open or close and accordingly, where electrically driven, require significant electrical power to actuate. The lock bolts on dead bolts in the larger safes are massive and require significant power to move. Whatever the large safe vault design, substantial power is required to unlock and open and to close and lock.

Traditionally, safes were unlocked or prepared for access by operation of a mechanical combination lock. The combination for access to the safe was set by a qualified locksmith. Each person with authorized access to the safe would be

furnished with the safe lock combination. The authorized person would then commit the operable lock combination to memory for later use.

In the event one of the authorized access persons left employment in the institution, or the access combination was believed compromised, the access combination had to be changed by a locksmith and all authorized persons were required to learn and memorize a new combination.

It is convenient to have a record identifying which authorized person entered the safe and the time of his or her entry. The mechanical combination lock with shared multi-person access makes it difficult to create or maintain accurate records of access events.

The appearance of secure electronic locks is a relatively recent development. Many electronic locks have been described in the patent literature, each of these earlier lock systems have been devised to provide one or more improved features such as recording each access event or, for example, providing less expensive change in the access code. However, none of these earlier electronic lock systems have been applicable to the unique set of high security yet convenient multiple person authorized access desired in larger high security safe vault installations.

## SUMMARY

The invention is comprised of multistage means for identifying and determining the authorization of a person attempting to enter a large safe entry barrier. The multiple stages include an access card means furnished each

authorized person, access card reader and keypad digital signal input means. A first microprocessor, the access card signal being entered into the first microprocessor. A control microprocessor, the keypad digital signal being entered into the control microprocessor. The first and control microprocessors having Read Only Memories (ROM) into which authorized identification codes are entered upon which identification codes may be matched or, if not matched, the access will be denied. Solenoid operated dead bolt locks are mounted upon the safe entry barrier. A source of high voltage DC electric power, electrical switch means for energizing the dead bolt solenoid to alternately assume an open position or a closed position by connecting the higher voltage DC electrical power source through the switch. The digital signal input derived from the control microprocessor provides information to control the switch means, whereby a massive safe solenoid lock may be operated while maintaining high security protocol.

## OBJECTS OF THE INVENTION

A first object of the present invention is to provide a highly secure electronic lock system having sufficient power adapted to unlocking and opening or securely locking a safe vault door having movable dead lock bolts.

Another object of the invention is to provide an electronic system for secure authorized multi-person user access to a safe installation.

Another object of the invention is to provide an electronic system utilizing both an access card and a numerical Personal Identification Number wherein the

secure lock system actuates using sufficient augmented electric power a solenoid-controlled dead bolt access control barrier to a safe installation.

Still another object of the invention is to provide an electronic secure lock system which provides inexpensive and readily executed changes in access codes for one or more of several authorized persons wherein such access code changes require no extensive mechanical safe lock adjustments.

Yet another object of the invention is to provide an electronic safe lock system for authorized access having means to provide sufficient electric power for large safe installations wherein the identity of the person and time of his or her authorized access is unambiguously recorded.

Other objects and advantages of the invention will be apparent from the following illustrations, specification, and claims.

## BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a diagram showing the component parts of a preferred embodiment of the invention.

Fig. 2 is a diagram showing the component parts of a preferred embodiment of the invention.

Fig. 3 is a diagram showing the component parts of a preferred embodiment of the invention.

Fig. 4 is a flow chart showing the flow of information during operation of the preferred embodiment of the invention illustrated in Fig. 1.

Fig. 5 is a flow chart showing the flow of information during operation of

the preferred embodiment of the invention illustrated in Fig. 2.

Fig. 6 is a flow chart showing the flow of information during operation of the preferred embodiment of the invention illustrated in Fig. 3.

Fig. 7 illustrates a variation of the preferred embodiment shown in Fig. 3.

## DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Referring to Fig. 1, which shows a schematic block diagram of a preferred embodiment of the invention, access sensor 100 is adapted to read code information input by a user seeking entry into the safe. The access sensor 100 comes in many forms today such as a magnetic card reader, input keyboard, biometrics scanner, bar code reader and holographic reader. The access sensor 100 design today is available in many packaged configurations of the aforementioned access sensor forms. Examples of such package configurations available are magnetic card reader and keyboard, bar code reader and keyboard and magnetic card reader and biometrics scanner. Any of the access sensor forms can be joined together to provide multiple layers of security. Access sensor 100 is directed by control element 110. Control element 110 is a programmable device that can receive input and respond to such input. An example of a control element in common use today is a microprocessor but any programmable device will work. The control element 110 can receive input from access sensor 100 and respond to the input in a programmed way. Control element 110 can also be programmed to initiate action on its own such as when a time-based sequence of

events is scheduled to occur. Control element 110 can send and receive information to both the access sensor 100 and voltage relay 120.

Fig. 4 shows the information flow through the embodiment represented in Fig 1. Block 400 shows that access codes are entered in the access sensor 100. In most cases, clients of the invention vender prefer at least two different types of codes to be entered for redundant protection, although both a single code and more than two codes is easily accommodated with what is conventionally available. Block 405 shows that entered information are recorded to provide a record for later auditing. Block 410 is where control element 110 analyzes the code entries. Block 415 is where control element 110 verifies that the codes match the codes on an accept list. Block 420 shows that when a set of codes are accepted, that a record of the date and time of the entry and which codes were accepted to allow the entry are recorded for later auditing purposes. Block 425 shows a signal is sent after the recordation of the entry to voltage relay 120. The signal sent to voltage relay 120 is a low voltage signal that does not provide enough power to drive solenoid 130. Consequently, voltage relay 120 turns on an alternate power supply to drive solenoid 130. The alternate power source is any conventional power source that provides enough power such as 120 or 220 volt AC current, DC battery supply or generator supply.

Referring to Fig. 2, which shows a schematic block diagram of a preferred embodiment of the invention, access code sensor 210 is adapted to read code information input by a user seeking entry into the safe. The access code sensor 210 comes in many forms today such as a magnetic card reader, biometrics

scanner, bar code reader and holographic reader. The access code sensor 210 design today is available in many packaged configurations of the aforementioned access sensor forms. Any of the access sensor forms can be joined together to provide multiple layers of security. Access code sensor 210 is directed by microprocessor 220. Microprocessor 220 is a programmable device that can receive input and respond to such input in a programmed way.

Fig. 5 shows the information flow through the embodiment represented in Fig 2. Block 500 shows that access codes are entered in the access code sensor 210. In most cases, clients of the invention vender prefer at least two different types of codes to be entered for redundant protection, although both a single code and more than two codes is easily accommodated with what is conventionally available. Block 505 shows that entered information are recorded to provide a record for later auditing. Block 510 is where microprocessor 220 analyzes the code entries. Block 515 is where microprocessor 220 verifies that the codes match the codes on an accept list. Block 520 shows that when a set of codes are accepted, keypad 200 is activated. When keypad 200 is activated, the person trying to gain entry to the safe has to enter a code on keypad 200. Block 530 shows that entered information is recorded to provide a record for later auditing. Block 530 is where microprocessor 220 analyzes the code entries. Block 540 is where microprocessor 220 verifies that the codes match the codes on an accept list. Block 545 shows that when a set of codes are accepted, that a record of the date and time of the entry and which codes were accepted to allow the entry are recorded for later auditing purposes. Block 550 shows a signal is sent after the

recordation of the entry to voltage relay 240. The signal sent to voltage relay 240 is a low voltage signal that does not provide enough power to drive solenoid 230. Consequently, voltage relay 240 turns on an alternate power supply to drive solenoid 230. The alternate power source is any conventional power source that provides enough power such as 120 or 220 volt AC current, DC battery supply or generator supply.

Referring to Fig. 3, which shows a schematic block diagram of a preferred embodiment of the invention, code sensor 300 is adapted to read numerical data encoded on the magnetic strip of a plastic access card. When a such an access card is swiped through the reader of code sensor 300, numerical data are transmitted to first microprocessor 310 which has a read-only memory (ROM), in which are contained allow access codes. If no match between the transmitted data and an access code is found, the program terminates and the display reads "access denied", while a match results in a display prompt reading "enter PIN". When a PIN is entered by means of a keypad 320, the entered data is transmitted to a control microprocessor 330 having a read-only memory (ROM) that compares the inputted PIN to a list of allowed PINS. No match results in termination of the program and a display prompt reading "access denied", while a match results in a display prompt such as "enter instruction code that requests a numerical code that will specific one or two electronic messages that result in sending a signal in the form of a 3 V pulse that passes through a voltage step up relay 350, into which 120 V AC flows after passing through an AC to DC converter 360, and then to solenoid 340 that controls the entry barrier.

Referring now to Fig.6, which shows the flow of information during operation of the preferred embodiment, access code sensor 600 reads data contained on an access card and transmits it to first microprocessor 310, where it is compared to allow codes stored in the ROM. A match prompts the user to enter a numerical PIN using keypad 320. The inputted PIN is transmitted to a control microprocessor 330 which records the inputted PIN and the time of the attempted entry and compares the inputted PIN to a list of ROM-stored allowed access PINs to determine whether a match exists. If a match exists, the display prompts the access seeker to enter numerical instructions. The input of a numerical instruction code results in a 3V signal being sent from the control microprocessor 330. This 3V signal is then amplified by 120V AC current passing through an AC to DC converter 360 to yield a 15V pulse which then actuates the solenoid.

Referring to Fig. 7 which shows a second embodiment of the invention that utilizes a spring loaded solenoid dead bolt access barrier, access card reader 10 and keypad 20 are combined in a wall amount unit 5. Display 30 instructs an access seeker to swipe an access card through access card reader 10. Upon swiping the card, the access code recorded on the card is transmitted to a first microprocessor 40, which compares it a list of ROM-stored access codes. If no match is detected, the program is terminated and the display 30 will read "access denied". If a match is detected, the display 30 instructs the access seeker to input a numerical PIN using keypad 20. The PIN is transmitted to a control microprocessor 50, having a Read Only Memory (ROM) in which are stored authorized PINs. The inputted PIN is compared to the authorized PINs, and if no

match is found, the program is terminated and display 30 will read "access denied." If a match is found between the inputted PIN and an authorized code, the display 30 will prompt the access seeker to give further instructions, which may include numerical codes for adjusting the time delay of the spring-loaded, solenoid controlled dead bolt barrier 60. A 3 volt pulse is then sent from control microprocessor 50 to voltage step-up relay 70 where it is amplified, perhaps by using an AC standby battery. Voltage step up relay then sends a 15 volt DC current to solenoid 80, which results in opening the dead bolt barrier 60 and compressing a spring 90. The dead bolt barrier 60 stays open until the period of the time delay expires. Following the expiration of the time delay, the spring is released, closing dead bolt access barrier.